

GS8 Modual Gateway User's Manual

Manual Part Number 96-00524-01



Zed-3
501 Valley Way
Milpitas CA 95035
USA

+1-408-587-9333
<http://www.zed-3.com>

Notice

The information contained in this document is subject to change without notice.

Zed-3 makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Zed-3 shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Zed-3 assumes no responsibility for the use or reliability of interconnected equipment that is not furnished by Zed-3.

This document contains proprietary information which is protected by copyright. The contents of this manual and the associated software are the property of Zed-3, and all rights are reserved. No part of this document may be photocopied, reproduced, stored in any computer format, translated to another language, or publicly displayed without the prior written consent of Zed-3.

The information contained herein has been prepared by Zed-3 solely for use by Zed-3's employees, agents, and customers. Dissemination or use of the information or concepts contained herein to or by other parties is prohibited without prior written consent from Zed-3.

Zed-3, the Zed-3 logo, the Zed-3 mark, GS8, CN2x2, CN2x4, SE150, SE150P, SE150+, SE150, SE500, and SEME are trademarks of Zed-3 and may be registered trademarks in certain countries. All other names may be trademarks or registered trademarks of their respective owners.

Revision History

Manual Release	Firmware Version	Release Date
1.0	1.0.0	13 June 2008
1.1	1.0.6.7	06 January 2009

Contents

Product Introduction	1
1.1 Product Introduction	1
1.2 Technical Specifications	1
1.3 Basic Features	3
1.4 Profile	3
1.5 Interface Module	5
Device Installation	7
2.1 Installation Requirements	7
2.2 Preparations	9
2.3 Installation Procedures	9
Web Management System	11
3.1 Login	11
3.2 Web Management System Interface	13
3.3 Menu Structure	14
Monitor	15
4.1 System Info	15
4.2 Line Status	16
4.3 Active Calls	18
4.4 Call Records	18
Line Settings	20
5.1 IP Line	21
5.2 GSM Line	23
5.3 CDMA Line	25
5.4 FXO Line	26
Call Settings	27
6.1 Matching Rules	27
6.2 Routing Matching Rules	28
6.3 Route	29
6.4 Alter	30
6.5 Filter	34
6.6 Schedule	36
6.7 System	38
Administration	40
7.1 Change Password	40

7.2	Network Setting	41
7.3	Time Setting.....	41
 SMS.....		44
8.1	Route.....	45
8.2	GTXT Client.....	47
8.3	Configuration	48
8.4	Send Test Message	50
8.5	Received Messages.....	50
 Maintenance		52
9.1	System Reboot.....	52
9.2	Config Management	52
9.3	Upgrade Firmware.....	53
9.4	Auto Attendant	54
9.5	Diagnostic Tools	55
 GS8 Disaster Recovery System.....		56
 Glossary		57

Chapter 1

Product Introduction

1.1 Product Introduction

Zed-3 GS8 is a Modular Gateway which has perfect performance, rich interfaces, and interface cards plug capacity. GS8 supports GSM/CDMA, SIP, FXO interface, so it can be connected with GSM/CDMA, VoIP and PSTN networks, allows calls to freely transfer between these interfaces. GS8 permits flexible call routing and call restriction settings to provide users calling strategy based on their own requirements. The web-based management platform dramatically reduces complication of users' operations.

GS8 are compatible with most SIP-based IP-PBX and traditional telephony system. When there is no PBX, it can be deployed alone or in a group. At the same time, this product can be connected to local PSTN network directly since it supports most countries and areas' telephone protocols. Zed-3 sales GS8 and provides technical supports over the world.

1.2 Technical Specifications

Specifications	Description
System capacity	- Up to 4 GSM ports(900/1800 MHz, 850/1900MHz) - Up to 8 FXO ports (loop start) - Any combination of interface cards 8 simultaneous calls
Hardware specification	1 reset button 4 extended slots 2 system indicator lights 2 LED per FXO card and GSM/CDMA card. - GSM/CDMA module: SMA connector - FXO module: RJ11 connector
Interface card capacity	4 extended slots 2-port FXO card 1-port GSM/CDMA card 1-port GSM/CDMA card
Network interface	one 10/100M LAN port
Voice capacity	- Codec: G.711 A-Law/U-Law?G.729?G.723.1 - Confort noise, voice activity detection, echo cancellation, jitter buffer. - DTMF Relay: In-band DTMF Relay, RFC-2833, SIP INFO
Physical characteristics	- Dimesion: 440mm x 225mm x 45mm (17.3"x8.9"x1.8") - Weight: 3.8kg (8.41 lb) - Power: AC-DC power adapter - Input: ATX PS,AC 100 ~ 240 V @ 47 ~ 63 Hz - Output: DC-5V - Power consumption: Max.20 Watt
Operating environment	- Operating temperature: 10 ~ 40 °C(50 °F ~ 104 °F) - Storage temperature: 0 ~ 50 °C(32 °F ~ 122 °F) - safety: meet - FCC Part 68 - electromagnetic interference: meet FCC Part 15A - RoHS: compatible

1.3 Basic Features

- Support SIP, meet RFC3261 standard, compatible with most SIP-based IP-PBXs
- Support flexible SIP calling, support connecting to other SIP devices like IP-PBXs in register or unregister way.
- Support GSM , CDMA and FXO interface via interface cards.
- Have Modular interface, support mix-plug of interface cards.
- Support flexible secondary dialing and DID function
- Support flexible call routing, freewill transfer between any two interfaces.
- Flexible call restriction.
- Powerful number transform includes head-trim, tail-trim, replacement, and number segment way.
- Full calling strategy management: set call schedule based on different time segments.
- Cascade and extend capacity in a unregister way
- Plenty system monitor: line status, current call, CDR, system status.
- Easy-use of web configuration and management system.
- Powerful safety management, upload/download configurations, fireware update, disaster recovery etc.

1.4 Profile

1.4.1 Appearance



Figure 1-1 GS8 appearance

1.4.2 Front View

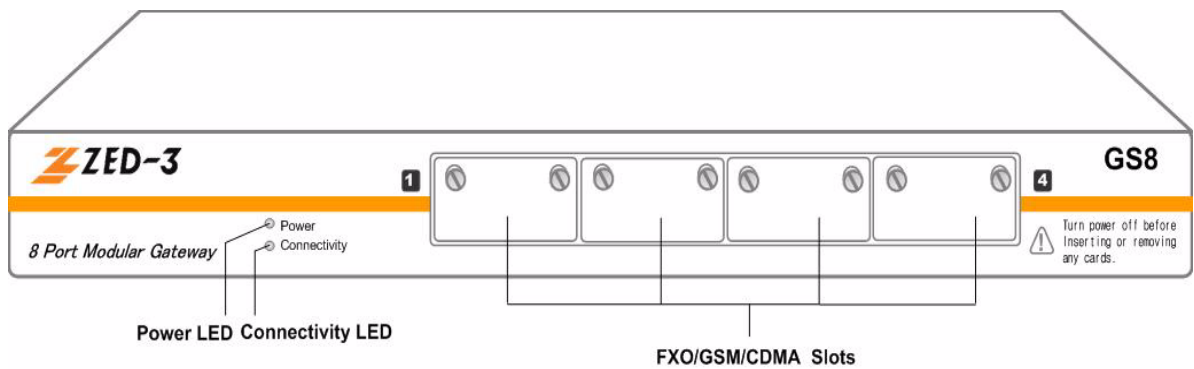


Figure 1-2 GS8 front panel

- Two LED indicators on the front panel of GS8 for system status:
 - **Power:** power indicator, be green when power-on.
 - **Connectivity:** network connectivity indicator.
 - * Be red if there is no Ethernet connectivity.
 - * Be orange if routing is blocked because of the failure of SIP subscriber register.
 - * Be green if any one of the trunks registered (by SIP) successfully.
- 4 extended slots which can hold two FXO cards and two GSM cards.

1.4.3 Back View



Figure 1-3 GS8 back panel

All ports here:

- **LAN port:** GS8 connects network via this port.
- **Reset button:** reset the configuration to factory defaults (includes network configuration). Press it for 6 seconds when system is running.
- **Power connectivity:** connect to power adapter.

1.5 Interface Module

GS8 has four extended slots which support three kinds of cards: GSM card, CDMA and FXO card. The mix is also supported.

One GSM card supports one GSM call, one CDMA card supports one CDMA call, but one FXO card has two FXO ports, so it supports two FXO calls. In total, GS8 supports eight FXO calls or four GSM calls or four CDMA calls.

1.5.1 FXO Interface Card

FXO interface card can be set on your PBX or telephone exchange SPC switch as an extension.

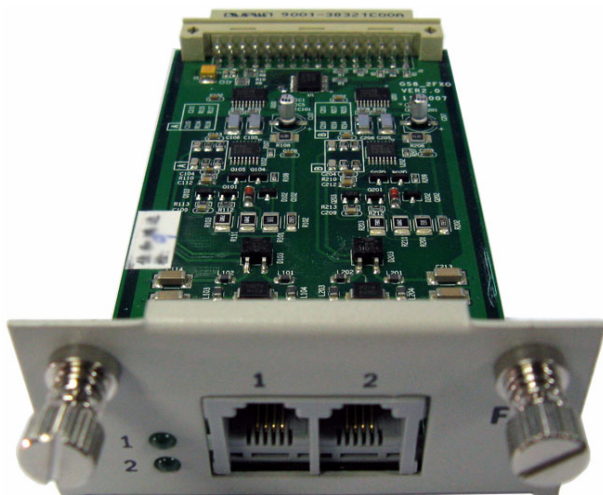


Figure 1-4 FXO interface card

There are two FXO ports and two indicators per FXO card, the corresponding light is on when the line is off-hook.

1.5.2 GSM/CDMA Interface card

GSM or CDMA interface modules: there are two LED lights to show running status:



Figure 1-5 GSM/CDMA interface card

- **Signal:** be red or green. be red if there is no signal. be off for 500ms then be red for 500ms if there is no SIM card. be orange when there is SIM card and signal but the register to service provider's network failed. be green if every thing is ok.
- **Service:** be red or green. be off if there is no call. be off for 500ms then be red for 500ms if there is no SIM card. be green when there is a call.

Chapter 2

Device Installation

Unpack the unit and verify shipment content with the packing list :

- One GS8 equipment.
- One power adapter and one power cable.
- One Ethernet cable.
- One copy of quick start guide.
- One copy of e-manual.
- One Zed-3 pen as a gift.
- Accessories package: six M6 screws, eight M4 screws, two GS8 fixers.

Note: If there is any missing or damage, contact the seller or Zed-3 sales immediately and save all packages for the repackaging if need.

2.1 Installation Requirements

2.1.1 Power Requirements

- Power-off before installation, dismantlement or movement.
- The electric outlet shall be installed near the equipment and shall be easily accessible in case of emergency.

2.1.2 Anti-static Requirements

- If the device's power line connects to external cable, take necessary anti-static actions please.
- Anti-static Requirements
 - Static will damage the circuit or the whole machine seriously if static exceed the limitation, so make sure the ground bus well enough.

- Static inside body will result in damage too, so please wear anti-static wristband if you have.

2.1.3 Environment Requirements

2.1.3.1 Basic Conditions

Keep the GS8 equipment in a room which has proper control of temperature and humidity, watch out the conductivity of the shelf. Too high or too low humidity will cause short circuit or fire. At the same time, the conductive property of rack is also considerable.

Place the equipment on a rack (if possible) which is near stable and liable power in an anti-fire, anti-humidity, anti-dust, and anti-thief room.

2.1.3.2 Temperature, Humidity, and Illumination

Suggestions:

- Temperature: 0 ~ 40
- Relative humidity: 5~ 95RH without coagulation
- Illumination: light, 500 ~750 lx, light enough for operations.

High humidity will affect the insulating efficiency of insulating materials and also cause the rust of metals. Low humidity will make insulating gasket shrink, loose the fixed bolts, and scrape up static. Long period of high temperature will accelerate components' aging, lower the reliability and reduce the useful time dramatically.

2.1.3.3 Air Quality

The air particulate may enter the equipment through ventholes. Too much dust will cause short-circuit, so the suggestion is less than 180mg/m³. In machinery room, printer and Photocopiers shall be placed away from the power provider in case of floating particulate. Please put it in the diagonal corner.

Keep the room clean, for the dust will cause static and bad connections between little components

2.1.3.4 Ventilation Requirements

There are thermal discharge holes in the back and side side, so keep more than 100mm from other stuffs for thermal discharging.

2.1.3.5 Safety

There must be some safety precautions like securities or other effective anti-thief actions. The lightning rod is well connected to the ground, the ground bus' diameter must be more than 5mm. For seismic zones, there must be anti-earthquake measurements, like fixed balustrade for the rack.

2.2 Preparations

2.2.1 Network Resources

GS8 shall be connected with intra-company network or Internet for different usages. Test your network connectivity and provide a port for this equipment. It is usually connected to a switch or a router.

2.2.2 IP Address

Get an IP address for your GS8. the setting of IP address, see 3.1.1set GS8's IP address.

Note: Static IP address is recommended, no matter public or private address. (except DDNS).

2.2.3 Ethernet Cable

Get a standard RJ-45 cable for GS8.

2.2.4 External Line

2FXO card is necessary if you want to call PSTN from GS8, connect its FXO port with PSTN with a cable.

Prepare a GSM card if you want to call mobile phones from GS8.

2.2.5 Other Soft-switch Accounts

Ask for soft switch accounts and register information like phone number, password, register proxy address, proxy address, register port, external proxy address, register expiration time etc.

2.2.6 Network Topology

Build your network topology based on GS8's location and connectivities.

2.2.7 Line Adjustment

Extend the external lines and cables to reach GS8's ports, if they are too far from the equipment.

2.3 Installation Procedures

GS8 equipment shall be placed on a table or a rack, install it as below steps.

Note: Do not put any heavy thing on the equipment to avoid any damage of the base.

2.3.1 Network Connection

Connect the cable with Ethernet LAN port on the back side.

2.3.2 Connect out Line

- Connect analog line with the port of 2FXO card on GS8
- If there is a GSM/CDMA card, connect an antenna with GSM/CDMA port. Better way is with a coaxial cable.
- If there are several wireless cards, these cards may share one public antenna.

2.3.3 Power Connection

1. Connect the power line with the power port on the back side.
2. Connect the other end with outlet nearby.

2.3.4 Power On

After all these steps, power on.

All LED indicators are off at the beginning, then the power indicator is green all the time.

Chapter 3

Web Management System

3.1 Login

Login to GS8 Web Server with IE browser (1024*768 recommended) and make configurations like this:

1. Open IE browser and enter IP address in the address field.

GS8 has a default address: 192.168.0.100. If the default address has been changed, gain it like below: (if you can not login, see 3.1.1 change GS8's IP address)

- Dial "****" and input password "23646" when you hear the dialing tone of AA after calling in through FXO port of GS8, and the equipment will show you the IP address. the SpreeCode and password used here are default, you may change them on the page of AA at **Call Settings-System Settings** after logging into the web management system.
- Or Press Reset button for 6 seconds and reset the configurations to the factory default (including the IP address recovered to default 192.168.0.100).

Note: The Reset button will reset all configurations, not only the IP address.

2. Input user name and password in the pop-up window. (see figure 3-1)

The image shows a web-based login interface for a device labeled 'GS8'. At the top left is a logo consisting of two interlocking keys. Below the logo, the text 'Please enter username and password.' is displayed. There are three input fields: 'Username' with the text 'admin', 'Password' with six dots, and 'Language' with a dropdown menu showing 'English'. A 'Login' button is located at the bottom center of the form.

GS8

Please enter username and password.

Username

Password

Language

Login

Figure 3-1 Login window

- Administrator: the default user name and password is "admin".

Change administrator's password in the **Administration > Change Password** menu after login.

3.1.1 Change GS8's IP Addresss

Any operation (including initialization) on configurations shall be made in the GS8's web management system. You can not login to the system if your PC's IP address does not belong to the same network segment as the equipment's. So the simplest way is to change your PC's IP address.

As below:

1. Change your PC's IP address to the same network segment (for example: 192.168.0.120)
2. Login to GS8: visit the default "192.168.0.100" with IE browser and login with "admin".
3. Click and enter **Administration> Network Setting** menu, change the IP Address, Net mask, Default gateway and DNS based on your real situation.

Figure 3-2 Change GS8's IP address

4. After setting, press **[Set]** button to make it work. roll your PC's IP address back.
5. Login to the web management system with the new IP address.

3.2 Web Management System Interface

There are six main menus on the top of the web management system's main page, they are **Monitor**, **Line Settings**, **Call settings**, **Administration**, and **Maintenance**.

Click each main menu to show its sub-menu, click the sub-menu to see the setting pages.

System Info	
Basic	
Model	GS8
Product ID	84B2FFA8D5A298D7D1FB0A6E4F4664D0
Firmware Version	1.0.6.7
Performance	
CPU Usage	22%
Memory Usage	32%
Time	
System Time	2008-12-16 11:59:23
System Uptime	18:38'16"
Latest Upgrade	2008-12-05
Network	
IP Address	10.0.0.244
Net Mask	255.255.255.0
Default Gateway	10.0.0.254
Primary DNS	198.41.0.4
Secondary DNS	202.106.0.20

Figure 3-3 Web Management System main interface

The system supports Chinese and English. Here is the English version.

3.3 Menu Structure

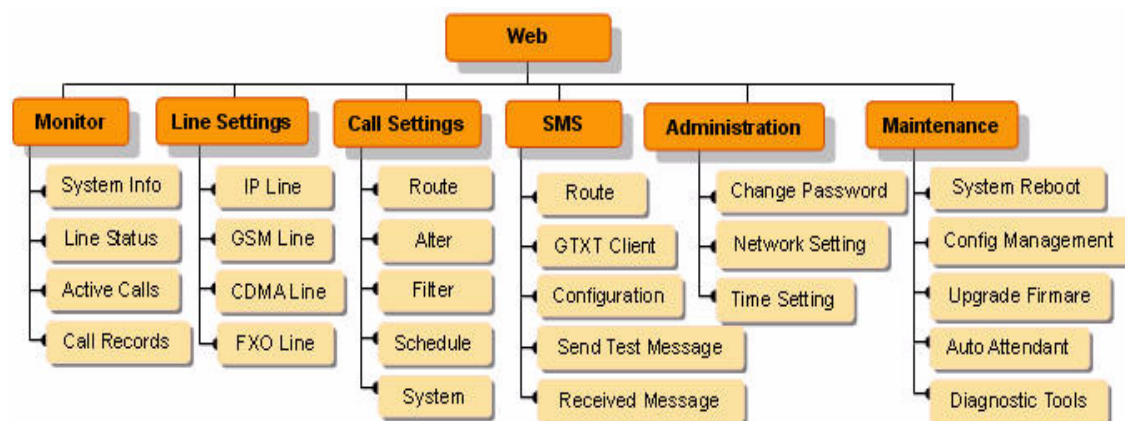


Figure 3-4 Menu Structure

Chapter 4

Monitor

The Monitor menu in Web Management System provides **System Info**, **Line Status**, **Active Calls**, **Call Records** etc..

4.1 System Info

Login to Web Management System or on the page of **Monitor > System Info**, there is system information about product model, firmware version, licence and resource usage etc.

Monitor	Line Settings	Call Settings	SMS	Administration	Maintenance
2008-10-28 16:34					
Common Tasks					
System Info					
Line Status					
Active Calls					
Call Records					
System Info					
Basic					
Model					
Product ID					
Firmware Version					
Performance					
CPU Usage					
Memory Usage					
Time					
System Time					
System Uptime					
Latest Upgrade					
Network					
IP Address					
Net Mask					
Default Gateway					
Primary DNS					
Secondary DNS					

Figure 4-1 System Monitor - System Info page

The parameters are:

- **Basic**

- **Model:** GS8.
- **Product ID:** the unique number of GS8 equipment.
- **Firmware version:** the current version of the equipment, like 1.0.6.7.
- **Performance**
 - **CPU Usage:** the current usage of CPU.
 - **Memory Usage:** the current usage of memory.
- **Time**
 - **System Time:** the current system time.
 - **System Uptime:** the duration from last start-up.
 - **Latest Upgrade Time:** the latest time of upgrade.
- **Network**
 - **IP Address:** the current IP address of the GS8 equipment.
 - **Net Mask:** the netmask now used.
 - **Default Gateway:** the IP address of the default gateway now used.
 - **Primary DNS:** the IP address of primary DNS now used.
 - **Secondary DNS:** the IP address of secondary DNS now used.

4.2 Line Status

Trunk lines are very important basic resources for GS8 system. All calls must have trunk lines to be made. GS8 has two kinds of trunk line: IP line and interface card line. You must use SIP protocol to make a call on IP line, you may add, delete, or modify IP line by yourself. Maximal capacity is 10 register IP lines and 10 unregistered IP lines. Interface card line is the lines which provided by interface card. Now we have GSM/CDMA and FXO cards. The number of interface card lines is fixed since the card is fixed, so you can not add, or delete any interface card lines, but only change the settings.

The system will monitor all these lines' status, and provide monitor information to the administrator for management.

Monitor > Line Status menu monitors all trunk lines, and classifies them into IP Line, PSTN Line and GSM/CDMA line as figure 4-2.

Type	ID	Phone Number	Status	Signal Strength (0~31)
GSM	slot1		Available	 <16>
GSM	slot2		No SIM Card	 <0>
CDMA	slot3		Available	 <31>
FXO	slot4-1		Invalid	
FXO	slot4-2		Invalid	
IP	1		Available	
IP	2		Available	
IP	4		Available	
IP	7		Available	

The signal strength must be at least 15 to have a reliable connection.

Figure 4-2 Monitor - Line Status page

- **Type** : the line type, includes: IP (Register IP or unregister IP), FXO , GSM/CDMA or GTXT.

Note: GTXT only shows registered GTXT (unregistered GTXT will not be shown). red font means unavailable line.

- **ID:** the sequence number of the line (for example: "slot1-2" means the 1st card's 2nd port).
- **Phone Number:** the phone number assigned to this line.
- **Status:** the status of the line
 - *For IP Line:* includes Available, Invalid, Full, Register fails, Registering.
 - *For GSM/CDMA line:* includes Available, Invalid, On used, Register fails, Registering, Signal low, No SIM Card
 - *For FXO line:* includes Available, Invalid, On used.

Note: GS8 monitors SIM cards of wireless modules (including GSM and CDMA), and all status will be shown at the Status field. For IP Line, GS8 checks whether unregister IP lines are ready every 10 minutes and shows the result at **Status** field.

- **Signal Strength(0~31):** the realtime signal checking of GSM/CDMA line, current scale is from 0 to 31. for example,  <16> means the signal magnitude is 16 and be checked every one minute.

The lowest level is 5, the signal less than 5 is showed as a blank, 5 to 9 shows one grid. 10 to 15 shows two grids. 16-20 shows three grids. 21 to 25 shows 4 grids. Greater than 25 shows full five grids.

4.3 Active Calls

Active Calls means the calls in conversations. The system provides real-time monitor of current calls. It's an important way of monitoring system for administrator.

Visit **Monitor > Active Calls** to see:

Caller	Callee	Callin Line	Callout Line	Status	Start Time
8888	62691416	IP/1	FXO/slot1-1	Talk	2008-11-17 14:59:07

Figure 4-3 Monitor -- ActiveCalls page

The fields are:

- **Caller:** the caller ID.
- **Callee:** the callee ID.
- **Callin Line:** the line type and port number of the caller in conversation, for example: "FXO/slot1-1" means the 1st port of the FXO card on the 1st port.
- **Callout Line:** the trunk type of the callee in conversation, for example: "GSM/slot4" means the GSM port which is in 4th slot.
- **Status:** the current status of the call.
- **Start Time :** the format is "YYYY_MM_DD HH:MM:SS".

4.4 Call Records

The system generates a detailed record (CDR) for every call. The CDR file will be saved automatically every day. The system will keep the newest 500 records when the data reached 30KB (about 700 records) limitation. Users can download CDR termly and clear them.

Caller	Callee	Callin Line	Callout Line	Status	Start Time	Duration
90003	77	IP/4	FXO/slot4-1	connected	2008-09-12 16:34:18	8"
90003	1002	IP/4	FXO/slot4-1	connected	2008-09-12 15:02:39	9"
90003	1002	IP/4	FXO/slot4-1	connected	2008-09-12 15:00:39	9"
90003	1002	IP/4	FXO/slot4-1	connected	2008-09-12 15:00:13	15"
90003	77	IP/4		in AA	2008-09-12 15:00:02	4"
90003	77	IP/4		route fail	2008-09-12 14:58:29	0"
	1002	FXO/slot4-1	IP/4	connected	2008-09-12 14:52:40	2'32"
		FXO/slot4-1		in AA	2008-09-12 14:52:10	20"
		FXO/slot4-1		in AA	2008-09-12 14:51:30	30"
	1002	FXO/slot4-1	IP/4	connected	2008-09-12 14:48:31	20"
	1002	FXO/slot4-1	IP/4	connected	2008-09-12 14:46:35	22"
		FXO/slot1-1		in AA	2008-09-11 10:03:06	20"
		FXO/slot1-1		in AA	2008-09-11 10:02:36	22"
15885652367	1002	GSM/slot2	IP/1	callee busy	2008-07-31 07:49:11	0"
15885652367	1002	GSM/slot2	IP/1	callee busy	2008-07-31 07:49:11	0"
15885652367	1002	GSM/slot2	IP/1	callee busy	2008-07-31 07:49:11	0"
15885652367	1002	GSM/slot2	IP/1	callee busy	2008-07-31 07:49:11	0"
15885652367	1002	GSM/slot2	IP/1	callee busy	2008-07-31 07:49:11	0"
15885652367	1002	GSM/slot2	IP/1	callee busy	2008-07-31 07:49:11	0"

Download Clear Page: 5

Figure 4-4 Monitor-Call Records Setting page

- **Caller:** the caller's phone number.
- **Callee:** the callee's phone number.
- **Callin Line:** the line type and port number of the caller in conversation, for example: "FXO/slot3-2" means the 2nd port of the FXO card which is in 3rd slot.
- **Callout Line:** the line type of the callee in conversation, for example: "GSM/slot4" means the GSM port which is in 4th slot.
- **Status:** the current status of the call, like in AA, no reply, routed fail etc.
- **Start Time:** the start time of the conversation.
- **Duration:** the duration in second of the conversation.

Chapter 5

Line Settings

Our GS8 equipment supports four types of interface cards: GSM, CMDA, FXO and IP card. On the page of **Line Settings** page, you can define the common properties of all kinds of lines in this equipment.

Monitor	Line Settings	Call Settings	SMS	Administration	Maintenance	admin
2008-10-28 17:16						
Common Tasks IP Line GSM Line CDMA Line FXO Line						
ID	Description	Phone Number	Register	Proxy	AA	
1	To MX250		Disable	10.100.100.99:5080	Disable	
2	To SE30+		Disable	10.100.100.21:5060	Disable	
4	To SE30P		Disable	192.168.200.52:5090	Enable	
7	To MX250		Disable	192.168.0.70:50202	Disable	

IP Settings

Description
 Register
 Proxy
 Registry Server
 Phone Number
 Username
 Password
 Register Expiration
 Home Domain
 NAT Traversal Mode
 Max Connections
 Enable AA
☐ Enable Backup Settings

Enable

 None

☐ Enable ☒ Disable

Figure 5-1 Line Settings page

5.1 IP Line

Here supports two ways of IP Line Settings: register and unregister.

For register-type IP Line, you need to set proxy's address and port, register server's address and port, user name and password, register expiration, NAT-traverse, home domain, and maximum connections and AA switch.

For unregister-type (P2P) IP Line, you need to set the counterpart's address and port, the maximum amount of calls, NAT-traverse, and AA switch etc.

5.1.1 IP Line List

- **ID:** the serial number of IP device, begins from 1.

Note: This number may not be the greatest since it may belong to the one deleted before.

- **Description:** the description of this line. (for backup configuration, this item is the same as the primary).
- **Phone Number:** the user name used when register.
- **Register:** enable or disable register server.
- **Proxy:** the IP address and port of the proxy.
- **AA:** enable or disable AA service.

5.1.2 Parameters Descriptions

- **Description:** the description of this device. (for backup setting, this item is the same as the primary one)

5.1.2.1 Registered IP Line

You need to set these when Register is "Enable":

- **Registry Server:** the IP address and port of registry server.

Note: The default port is 5060 if you set only IP address.

- **Proxy:** the IP address and port of the proxy.

Note: The default port is 5060 if you set only IP address.

- **Phone Number:** the phone number of this line.
- **Username :** the user name for register

- **Password:** the password for register.
- **Register Expiration:** timeout after these seconds.
- **Home Domain:** domain's IP address.
- **NAT Traversal Mode:** three modes:
- **None:** no mode.
- **Port Forwarding:** port forwarding mode:
- **Public Address:** set public IP address or domain and port, the IP and port are separated by ":".
- **Outbound:** the IP address and port of the Outbound proxy which is typically used in an environment with a firewall/NAT for signals and media stream traverse firewall/NAT.
- **Outbound Proxy:** set IP address or domain and port for outbound proxy, the IP and port are separated by ":".

Note: The default port is 5060 if you set only IP address.

- **Max Connections:** maximal simultaneous call number supported.
- **Enable AA:** if enter AA (Auto Attendant) when dial in via this line.

5.1.2.2 Unregister IP Line

Set these paramters when Register is "Disable":

- **Proxy:** the same as 5.1.2.1 IP Line
- **Phone Number:** the same as 5.1.2.1 IP Line
- **Username:** the same as 5.1.2.1 IP Line
- **Password:** the same as 5.1.2.1 IP Line
- **Ping Interval:** for unregister IP Line, you may set Ping Interval to let system Ping it periodically for its status. When the value is 0, the system does not Ping it and think it available for ever.
- **NAT Traversal Mode:** the same as 5.1.2.1 IP Line
- **Max Connections:** the same as 5.1.2.1 IP Line
- **Enable AA:** the same as 5.1.2.1 IP Line

Note: If there is no callerID when call out via unregister IP Line, the default Caller ID is 1111.

5.1.3 Backup Settings

Set parameters for backup proxy for registered IP Line. All items are the same as the primary.

☒ Enable Backup Settings

Backup Settings

Proxy	
Registry Server	
Phone Number	
Username	
Password	
Register Expiration	
Home Domain	

Figure 5-2 Line Settings - Backup Setting page

5.1.4 Add IP Line

1. Filling the blanks in the edit area, or check ☒ **Enable backup settings** to use the backup configuration.
2. Press **[Add]** and the new record will appear on the list.

5.1.5 Edit IP Line

1. Click a record on the list.
2. Modify the parameters in the edit area, or modify the backup configuration.
3. Press **[Modify]** and save it. The list is updated immediately.

5.1.6 Remove IP Line

1. Choose a record on the list.
2. Press **[Remove]** and save it.

5.2 GSM¹ Line

If the IP-PBX has GSM card, the web management system will show your GSM line setting page.

5.2.1 GSM Line List

- **ID:** the slot number of GSM device, like "slot1".
- **Phone Number:** the phone number of this line.

1. Show this parameter when GS8 has GSM module.

ID	Phone Number	AA
slot4		Enable

Phone Number

Enable AA

☐

Output Volume

Normal

Input Volume

Normal

Voice In Call

No

Working Frequency

900/1800MHZ

Modify

Figure 5-3 Line Settings - GSM Line Settings page

- **AA:** the status of AA: enable or disable.

5.2.2 Parameters Descriptions

- **Phone Number:** the phone number of this line
- **Enable AA:** If enter AA (Auto Attendant) when dial in via this line.
- **Output Volume:** Output volume of this line: low, middle, high, highest.
- **Input Volume:** Input volume of this GSM line: low, middle, high, highest.
- **Voice In Call:** Accept or reject returned voice when call out via this line.
- **Working Frequency:** Working frequency of this GSM line.

You may use different type GSM module on GS8.

- Working Frequency is gray and un-configurable when GSM use double frequencies: 900 / 1800 MHZ.
- There are 3 frequency segments when GSM module is four frequencies module: 900/1800MHZ, 850/1900MHZ, 900/1900MHZ

5.3 CDMA² Line

If the IP-PBX has CDMA card, the web management system will show your CDMA line setting page.

ID	Phone Number	AA
slot3		Enable

Phone Number

Enable AA

☐

Output Volume

Normal ▼

Input Volume

Normal ▼

Voice In Call

No ▼

Modify

Figure 5-4 Line Settings - CDMA Line Settings page

5.3.1 CDMA Line List

- **ID:** The slot number of GSM device, like "slot3" which means the 3rd interface card is CDMA module.
- **Phone Number:** The phone number of this line.
- **AA:** the status of AA: enable or disable.

5.3.2 Parameters Descriptions

- **Phone Number:** The phone number of this line
- **Enable AA:** If enter AA (Auto Attendant) when dial in via this line.
- **Output Volume:** Output volume of this line: low, middle, high, highest.

2. Show this parameter when GS8 has CDMA module.

- **Input Volume:** Input volume of this GSM line: low, middle, high, highest.
- **Voice In Call:** Accept or reject returned voice when call out via this line.

5.4 FXO Line

If the IP-PBX has FXO card, the web management system will show your FXO line setting page.

ID	Phone Number	AA
slot1-1	9000	Disable
slot1-2	9000	Disable

Phone Number

Polarity Reversal

☐ Enable
 ☒ Disable

Enable AA

☐

Figure 5-5 Line Settings - FXO Line Setting page

5.4.1 FXO line List

- **ID:** the real position of FXO interface card on GS8, like "slot2-1" which means the 1st FXO interface card on the 2nd slot is FXO module.
- **Phone Number:** the phone number of this line.
- **AA:** the status of AA, enable or disable.

5.4.2 Parameters Descriptions

- **Phone Number:** The phone number of this line.
- **Polarity Reversal:** If enable Polarity Reversal function.
- **Voice In Call:** Accept or reject returned voice when calling out via this line.
- **Enable AA:** If enter AA (Auto Attendant) when dialing in via this line.

Chapter 6

Call Settings

The **Call Settings** menu of Web Management System provides configurations of call routing, number transform, call filtration, schedule group, and system configuration. Among them, number transform, call routing and call filtration co-exist and supplement each other. Call routing is the core, plus number transform, call filtration, numbering plan and schedule setting, all of them are combined to provide flexible control of coming and going calls via GS-8 modular gateway.

6.1 Matching Rules

Matching rules of numbers are one base of call routing, number transform and call filtration. So let's begin with these matching rules. The definition of these rules which we used refers to Digit Map (refers to RFC3435). 18 characters are valid: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, X?or x?, [,] , " , ' , - , " . , # , * , as below.

Pattern	Description
0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 0, *, #	One button on the phone panel
[m-n]	It's a scope. $m \leq n$. if $m = n$, it's [M] , means one number. If m or n is invalid, the system replaces m-n with a 'X' means a digit from 0 to 9.
[0-2,5,7-9]	More than one scope separated with comma composes a union. Every single scope's explanation is like above. If some scopes have cross-cutting areas, take the final union area.
X	A digit from 0 to 9, like 0X58 or 0x78. 'X' is case-unsensible.
.	One or more-than-one digit from 0 to 9, like 0x2

Examples:

<i>Input</i>	<i>Output</i>
• 1234X	The first four digits are 1234, the fifth is a digit from 0 to 9, five digits totally.
• 1234[1,5-9]	The first four digits are 1234, the fifth is 1 or a digit from 5 to 9, five digits totally.
• 1234.	Any number begins with 1234.
• 1234[1,5-9].	The first four digits are 1234, the fifth is a digit from 0 to 9, the sixth is 1 or a digit from 5 to 9, followed by any number of any length.
• [1,3,6,8-9]	A digit which is 1, 3, 6, or a digit from 8 to 9.
• ##	Special character #.
• *xx	Start with * and followed by two-digit number.

Matching principle:

Please pay attention to the way of matching, all number rules should be completely matched. For example, the rule '800' will only match the number of 800, but not 8008108888. If what you want is 8008108888, the rule should be '800XXXXXXX' or '800.'

6.2 Routing Matching Rules

Note: Number transform and Call filtration follows the same rules:

1. Compare Source Line first, matching Line ALL (like: P/ALL?GSM/ALL?FXO/ALL etc.) is basic matching (with low level). Specific Line is perfect matching (with high level), and choose a line with the highest level.
2. Compare Caller Pattern if there are more than 1 lines with the same level, rules are:
 - a. Matching callerID and Caller Pattern of this route.
 - b. If the same-positioned digit is matched, match value add to 1.
 - c. "." means matching one digit from this and following digits.
 - d. Match one digit if Caller Pattern is empty; choose a higher level route in the results.
3. Compare Callee Pattern if there are more than 1 routes after 2, the rules are the same as 2.
4. Choose the top posting one if there are more than 1 routes after 3.

6.3 Route

Call Settings > Route lists trunks available and decides which record to use and how to control the calls based on source device, caller id, callee id and call time etc.

Call Settings page is separated into two areas: the list area and the edit area:

- The list area: show the created route list
- The edit area: configure routes here.

Monitor	Line Settings	Call Settings	SMS	Administration	Maintenance	admin	Logout
2008-11-06 15:33							
Common Tasks Route Alter Filter Schedule System							
Description	Source	Destination	Caller Pattern	Callee Pattern	Schedule		
SE500toFXO	IP/1	FXO/ALL	ALL	ALL	NULL		
FXOtoSE500	FXO/ALL	IP/1	ALL	ALL	NULL		
GSMtoSE500	GSM/ALL	IP/1	ALL	ALL	NULL		
SE500toGSM	IP/1	GSM/ALL	13501394905	ALL	NULL		

Description

Source Line

FXO ☐ ALL ☐ slot1-1 ☐ slot1-2
 GSM ☐ ALL ☐ slot4
 IP ☐ ALL ☐ 1

Caller Pattern

Callee Pattern

Schedule

Destination Line

FXO ☐ ALL ☐ slot1-1 ☐ slot1-2
 GSM ☐ ALL ☐ slot4
 IP ☐ ALL ☐ 1

Figure 6-1 Call Settings - Route page

6.3.1 Call Route List

The list shows a group of configured routes based on the creation time. The system will match the route table with current call information until the system find the proper route.

- **Description:** the description of this route.
- **Source:** the type of the source device and ports available.

Note: The principle of routing we used here is Perfect Matching, which is searching the most matched route based on source line. For example, there are two routes, the Sources of route A are IP1 and IP2, the Source of route B is IP1, so when a call is from IP1, no matter which route is on the first position, the system will choose route B.

- **Destination:** the type of the destination device and ports available.
- **Caller Pattern:** caller number need to be matched for this call. the default is 'ALL'.
- **Callee Pattern:** callee number need to be matched for this call. the default is 'ALL'.
- **Schedule:** the valid time segment, the default is 'NULL' means no time segment limitation.

Choose one route and click **[Move Down]** or **[Move Up]** buttons to reorder the sequence. click **[Modify]** or **[Remove]** button to edit or delete routes.

6.3.2 Parameters Descriptions

Enter necessary parameters in edit area when you create a new route, press **[Add]** and save it.

Note: You can not call if there are no routes.

- **Description:** the description of this route.
- **Source Line:** the type of source device (includes FXO, GSM, CDMA, IP) and ports available (multi-chosen). For example, 'Slot1-2' means the 2nd port of the 1st card. "G/C" means GSM or CDMA module: C-slot3 is the CDMA port of the third interface card, "G-slot4" is the GSM port of the fourth interface card.
- **Caller Pattern:** the number pattern of caller (see 6.1 number matching rules), the default is all patterns are valid.
- **Callee Pattern:** the number pattern of callee (see 6.1 number matching rules), the default is all patterns are valid.
- **Schedule:** the valid time segment of this route. Default 'NULL' means no time limitation. The schedule is set in Schedule menu (see 6.5 Schedule Group)
- **Destination Line:** the type of destination device (includes FXO, CDMA, GSM, IP) and ports available (multi-chosen), default 'ALL' means all ports of this card can be used.

6.4 Alter

Alter is the translation of call numbers based on different strategies. For example, strip ahead or behind, add ahead or behind, part-replace or all-replace. There are created alter rules based on created time in the list. In process, the system will match this rule list with current call information until find the perfect one.

The list area and the edit area of this page:

- The list area: show established list of number transform.

- The edit area: the edit area of settings.

Description	Type	Source	Destination	Caller Pattern	Callee Pattern	Schedule
	post	IP/1	GSM/ALL	ALL	ALL	NULL

Description

Type

Pre-routing ▼

Source Line

FXO ☐ ALL ☐ slot2-1 ☐ slot2-2
GSM ☐ ALL ☐ slot1
IP ☐ ALL ☐ 1

Caller Pattern

Callee Pattern

Alter Strategy

Edit

Schedule

NULL ▼

Add Modify Remove Move Down Move Up

Figure 6-2 Call Settings - Alter page

6.4.1 Alter Strategies List

Alter strategies list shows you a group of created strategies. GSM supports transforming multi-number based on one matching mode.

- **Description:** the description of this transform strategy.
- **Type:** the execute mode of this strategy: pre-routing or post-routing.
- **Source:** the type of source device and ports available
- **Destination:** the type of destination device and ports available
- **Caller Pattern:** caller number need to be matched for this rule, the default is 'ALL'
- **Callee Pattern:** callee number need to be matched for this rule, the default is 'ALL'
- **Schedule:** the valid time segment of this strategy, default 'ALL' means no time limitation.

Choose one strategy and press **[Move Down]** or **[Move Up]** buttons to reorder the sequence. press **[Modify]** or **[Remove]** buttons to edit or delete this strategy.

6.4.2 Parameters Descriptions

Enter necessary parameters in edit area when you create a new strategy, press Add button to save it.

- **Description:** the description of this strategy.
- **Type:** the execute mode of this strategy: Pre-routing or Post-routing.

Number transform can be done in two periods: before routing (pre-routing) and after routing (post-routing). Pre-routing will effect on the determination of call routing. post-routing alter numbers after routing, which will not affect the progress of routing, but will affect the way of call filtration, because post-routing call filtration is always behind number transformation.

Note: If you select 'post-routing', please set 'Destination line List'.

- **Source Line:** the type of source device (includes FXO, GSM, IP) and ports available (can be multi-chosen) , for example, 'Slot1-2' means the 2nd port of the 1st card.
- **Caller Pattern:** the number pattern of caller (see 6.1 number matching rules). No setting means all patterns are valid
- **Callee Pattern:** the number pattern of callee (see 6.1 number matching rules). No setting means all patterns are valid
- **Alter Strategy:** specific transform rules. For more details, see 6.3.3 number transform rules.

Note: In **Alter Strategy Settings**, it's composed of several sub-strategies (up to eight sub-strategies), and these sub-strategies are order-sensitive, please be careful about it.

Order	Enable	Caller	Strip	Head	Parameter
1	☐	Caller	Strip	Head	
2	☐	Caller	Strip	Head	
3	☐	Caller	Strip	Head	
4	☐	Caller	Strip	Head	
5	☐	Caller	Strip	Head	
6	☐	Caller	Strip	Head	
7	☐	Caller	Strip	Head	
8	☐	Caller	Strip	Head	

OK

Figure 6-3 Call Settings - Alter Strategy Settings page

- Transform Objective: caller or callee number.
- Transform action: includes Strip, Add, Keep, Replace, Calculate.
- Transform location: head or tail.
- Transform parameter: digit number or specific number or string etc. press OK to save it and exit.
- **Schedule:** the valid time segment of this route, the default is 'NULL' means no time limitation. Schedules are set in Schedule Group menu (see 6.5 Schedule Group).
- **Destination Line:** the type of destination device (includes FXO, GSM, IP) and ports available (can be multi-chosen) , for example, 'ALL' means all ports are available. When the **Type** is post-routing, you need to set this destination line.

6.4.3 Alter Rules

The rules are:

- **Strip caller or callee number from head:** strip **N** digits from the head of caller or callee number. **N** must be equal to or more than 1 ($N \geq 1$). If **N** is more than the length of the caller or callee number, give up this operation. For example: strip 3 digits from the head, 01082356031 becomes 82356031.
- **Strip caller or callee number from tail:** strip **N** digits from the tail of caller or callee number. **N** must be equal to or more than 1 ($N \geq 1$). If **N** is more than the length of the caller or callee number, give up this operation. For example: strip 3 digits from the tail, 95588123 becomes 95588. But this function is seldom used.
- **Add a prefix to caller or callee number:** add a **N** digits prefix on the head of caller or callee number and make a new number. **N** must be equal to or more than 1. For example: pre-pend '17909' to '02088786688', so the final number is '1790902088786688'.
- **Add a postfix to caller or callee number:** add a **N** digits postfix on the tail of caller or callee number and make a new number. **N** must be equal to or more than 1. For example: append '.7788' to '02088786688', so the final number is '02088786688,7788'.
- **Keep N digits from the head of caller or callee number:** keep **N** digits from the head of caller or callee number. **N** must be equal to or more than 1. If **N** is more than the length of number, keep it completely. For example: keep 5 digits from the head of '9558823423453451311', it should be '95588'
- **Keep N digits from the tail of caller or callee number:** keep **N** digits from the tail of caller or callee number. **N** must be equal to or more than 1. If **N** is more than the length of number, keep it completely. For example: keep 4 digits from the tail of '010887866887007', it should be '7007'.
- **Replace caller or callee number:** replace caller or callee number with a completely different number. For example: replace '10086' with '10088'.
- **Replace N digits from the head of caller or callee number:** replace **N** ($N \geq 1$) digits from the head of caller or callee number with another number. If **N** is more than the length of caller or callee number, replace the number with another different number completely. For example: replace 3 digits from the head of '10086' with '200', it should be '20086'.

- **Replace N digits from the tail of caller or callee number:** replace **N** ($N \geq 1$) digits from the tail of caller or callee number with another number. If **N** is more than the length of caller or callee number, replace the number with another different number completely. For example: replace 2 digits from the tail of '10086' with '68', it should be '10068'.
- **Calculate the last N digits of caller or callee number with an integer I:** add an integer **I** to the last **N** digits of caller or callee number and gain a new number. **I** should be equal to or more than negative 9999, and be equal to or less than 9999 ($-9999 \leq I \leq 9999$). This action only works on the last 4 digits of the phone number and does not care the carry. For example: the old extension numbers are from 7001 to 7050, another system has a segment from 2301 to 2350, you may execute $I = -4700$ to reflect these two segments.

For example:

1. Redirect all the calls from FXO1 line to 7777 of IP-PBX 192.168.11.22, the others to 8888. (Redirect calls to IP-PBX is routing, 8888 is the result of number transform, which change the callee number to 8888)
2. Redirect the caller '13910122334' from FXO1~4 line to 8888 of IP-PBX 192.168.11.22. (Redirect to IP-PBX 192.168.11.2 is routing, 8888 is the result of number transform, which change the callee number to 8888)
3. Redirect all calls from GSM1~2 line during off-work time to 9999 of IP-PBX. (Redirect to IP-PBX is routing, 9999 is the result of number transform, which change the callee number to 9999)

6.5 Filter

Call filtration determines what kind of calls is allowed to get through the gateway. It looks like some black and white lists. There are some parameters and strategies. There are created filter rules based on the created time. In process, the system will match this rule list with current call information until find the perfect one. There is at least one rule which is the default one that can be changed but not removed.

The page has two areas: the list area and the edit area:

- The list area: show the call filtration list.
- The edit area: set the parameters of call filtration record.

Description	Type	Source	Destination	Caller Pattern	Callee Pattern	Schedule	Strategy
default	pre			ALL	ALL	NULL	accept

Description

Type

Pre-routing

FXO

☐ ALL

☐ slot2-1

☐ slot2-2

Source Line

GSM

☐ ALL

☐ slot1

IP

☐ ALL

☐ 1

Caller Pattern

Callee Pattern

Strategy

Accept

Schedule

NULL

Add

Modify

Remove

Move Down

Move Up

Figure 6-4 Call Settings - Call Filtration Setting page

6.5.1 Filter List

Call filtration matching strategy is similar with route matching strategy. From up to down, get the first matched strategy no matter how many strategies left are matched too. Then determine whether let this call via the gateway based on this strategy's filtration action.

- **Description:** the description of this filter strategy.
- **Type:** the execution type of this filter strategy: pre-routing or post-routing.
- **Source:** the type of source device and ports available.
- **Destination:** the type of destination device and ports available.
- **Caller Pattern:** caller number need to be matched when use this rule, the default is 'ALL'
- **Callee Pattern:** callee number need to be matched when use this rule, the default is 'ALL'
- **Schedule:** the valid time segment of this strategy. The default is no limitation. The schedule is set in Schedule (see 6.5 Schedule Group).
- **Strategy:** the action of this strategy.

Choose one strategy on the list, press **[Move Down]** or **[Move Up]** button to reorder the sequence. press **[Modify]** or **[Remove]** button to edit or delete this strategy.

6.5.2 Parameters Description

Set parameters in edit area when you create a new strategy. Press **[Add]** button to save it.

- **Description:** the description of this strategy.
- **Type:** the execute mode of this strategy: pre-routing or post-routing.

Call filtration can be used in two locations: before number transforming before routing (pre-routing) and after number transforming after routing (post-routing). Pre-routing mode stops some calls before they are transformed before routing. post-routing mode stops some calls after they are transformed after routing. For most stoped calls, they are stoped before routing, and post-routing mode is an extended feature.

Note: If you choose 'post-routing' mode, please set 'destination line list' first.

- **Source Line:** the type of source devices (includes FXO, GSM, CDMA, IP) and ports available(may be multi-chosen). For example: 'Slot1-2' means the 2nd port of the 1st card.
- **Caller Pattern:** the pattern of caller number (pattern's rule, see 6.1 number matching rules). Blank means all patterns are valid.
- **Callee Pattern:** the pattern of callee number (pattern's rule, see 6.1 number matching rules). Blank means all patterns are valid.
- **Strategy:** the action of this strategy: Accept or Drop.

Note: There are two default strategies you can choose. They are 'accept all calls' and 'drop all calls'

- **Schedule:** the valid time segment of this strategy. 'NULL' means no limitation.
- **Destination Line:** the type of destination devices (includes FXO, GSM, CDMA, IP) and ports available (may be multi-chosen). For example: 'ALL' means all ports of this card are available. You need to set it if you select 'post-routing' mode.

6.6 Schedule

All time segments used in Call Settings are managed here. In this menu, you can add, edit or delete time segment.

6.6.1 Add a Schedule

There is no record in time segment list here when you first set it. click **'Add ...'** to create a schedule and specify details of the schedule.

Note: Create a group before you add a schedule, and set specific time after group creation.

6.6.1.1 Add a Group

Schedule Group	Properties
Add...	

Figure 6-5 Call Settings - Schedule Group Settings page

1. Press '**Add ...**' under **Schedule Group** to enter the page.

Parameters here:

- **Description:** the description of this schedule.
- **Date Range Type:** the range type of date: by day, by week, by month, by year, work day or every day.
- **Time range:** the specific time range.

Adding schedule group...

Description:

Date Range Type:

☒ By Day
☐ By Week
☐ By Month
☐ By Year

☒ Work Day
☐ Every Day

Time range:

Time range From: To:

[Add](#)

Figure 6-6 Call Settings - Add Schedule Group Settings page

2. Click [**Add**] to save it.

6.6.1.2 Add a Schedule

1. Press '**Add ...**' to enter the page

Schedule Group Properties				
	Description	Time Range	Info	Action
1 Remove	GROUP1	0800-1800	WORKDAY	Modify Remove
	Add...			
	Add...			

Figure 6-7 Call Settings - Add Schedule Setting page

The parameters are:

- **Description:** the description of this schedule
- **Date Range Type:** the range type of date: by day, by week, by month, by year, work day or every day.
- **Time range:** the specific time range

2. Click **[Add]** to save it.

6.6.2 Schedule Management

Use **'Modify'** , **'Remove'** to change or delete existing schedule in the list.

6.7 System

Configurations about VoIP services are set in **System** menu.

System Settings

SIP

Local SIP Port: 5060

Local RTP Port: From 31000 To 32000

DTMF Mode: RFC2833

Telephone Event: 101

Codecs: Unselected (empty box) --> Selected (ulaw, alaw, g729, g723) <--

Timer

Timer for Ringing: 10 Seconds

Timer for No Answer: 180 Seconds

Timer for RTP Detection: 180 Seconds

AA

Dial Mode: Both

Dial End String: #

Dial Timeout: 3

Query IP: ***

Auth Enable: ☒ Enabled ☐ Disabled

Auth Password: 23646

FXO

Tone Zone: China

CID Type: FSK

Set

Figure 6-8 Call Setings - System Settings page

6.7.1 SIP

- **Local SIP Port:** SIP listening UDP port.
- **Local RTP Port :** RTP UDP ports range.
- **DTMF Mode:** RFC2833?SIP INFO message, or in-bound mode.
- **Telephone Event:** the payload type of telephone event code.
- **Codecs: codecs supported :** g723, g729, ulaw, alaw. The default sequence is g711u, g711a, g729, g723 seperated by comma.

6.7.2 Timer

- **Timer for Ringing:** how long wait for ringback after dialing out.
- **Timer for No Answer:** how long wait for the answer after dialing out and receiving ringback.
- **Timer for RTP Detection:** the default value is 180, the range is from 10 to 3600, count in second.

6.7.3 AA

- **Dial Mode:** dial mode, includes Dial End String, Dial Timeout or Both.
- **Dial End String:** the default is #.
- **Dial Timeout:** expiration time of dialing, count in second.
- **Query IP:** how to get GS8's IP address, composed by 12 keys : 0-9, *, #, the default is "****", see 3.1 Login.
- **Auth Enable:** if need authentication information when querying GS8's IP address. If yes, you should set Auth Password also. The default is 23646, see 3.1 Login.

6.7.4 FXO

- **Tone Zone:** ring character for local country or area (different country or area has different ring frequency, length, or interval), GS8 provides 36 common ring solutions for your convenience.
- **CID TYPE:** coming call display type of FXO line: FSK, ETSI DTMF, India DTMF, Brazil DTMF. You need to ensure the both **CID TYPE** are the same mode when GS8's FXO connects to the peer. The receiving of CID caller number will be affected if not.

Chapter 7

Administration

You may use this menu to change administrator password, and manage system time and network settings.

7.1 Change Password

Change the administrator's password here, (other users' passwords are set in **Administration > Change Password**)

- **Current Password:** the password now used.
- **New Password:** the new password.
- **New Password (confirmed):** input the new password again.

Monitor	Line Settings	Call Settings	SMS	Administration	Maintenance
2008-11-17 13:32					
Common Tasks					
Change Password					
Network Setting					
Time Setting					
Administrator Password					
Current Password					
New Password					
New Password (Confirmed)					
Set					

Figure 7-1 Administration - Change Password Settings page

Note: Input the new password twice to confirm it.

7.2 Network Setting

Click **Network Setting** on the left task bar to set the work mode of LAN, IP address, netmask, default gateway, DNS server, and enable or disable VLAN.

Figure 7-2 Administration - Network Settings page

- **Work Mode:** two work modes: static or DHCP.
 - DHCP mode.
 - In Static mode, you need to set these parameters:
 - * **IP Address:** the local IP address.
 - * **Net Mask:** the netmask of subnet.
 - * **Default Gateway:** the default gateway of subnet.
 - * **Primary / Secondary DNS:** the IP address of primary or secondary DNS server.
 - * **VLAN:** enable or disable VLAN.

You need to set GS8's **VLAN tag** if you enabled VLAN, GS8 will send IP package with VLAN tag.

The configuration refers to 3.1 change GS8's IP Address.

Note: Press [Set] button to save the configuration.

7.3 Time Setting

In **Administration > Time Setting** menu, you can set the way of time acquiring: via NTP server or set it by yourself.

If you use NTP server, please set right time zone and NTP server (with domain or IP address) to get the correct time.

Set it by yourself, be careful about the format: YYYY-MM-DD HH:MM:SS.

7.3.1 Enable Time Server

Set NTP server to synchronize the system time of the equipment.

Note: If the equipment synchronizes time with NTP server, please set right time zone and NTP server (with domain or IP address) to get correct time.

Time Setting

NTP ☒ Enabled ☐ Disabled

NTP Server

Update Interval

Time Zone

- (GMT+04:30)Kabul
- (GMT+05:00)Ekaterinburg
- (GMT+05:00)Isamabad, Karachi, Tashkent
- (GMT+05:30)Chennai, Kolkata, Mumbai, New Delhi
- (GMT+05:30)Sri Jayawardenepura
- (GMT+05:45)Kathmandu
- (GMT+06:00)Almaty, Novosibirsk
- (GMT+06:00)Astana, Dhaka
- (GMT+06:30)Yangon(Rangoon)
- (GMT+07:00)Bangkok, Hanoi, Jakarta
- (GMT+07:00)Krasnoyarsk
- (GMT+08:00)Beijing, Chongqing, HongKong, Urumqi**
- (GMT+08:00)Irkutsk, Ulaan, Bataar
- (GMT+08:00)Kuala Lumpur, Singapore
- (GMT+08:00)Perth
- (GMT+08:00)Taipei
- (GMT+09:00)Osaka, Sapporo, Tokyo
- (GMT+09:00)Seoul
- (GMT+09:00)Yakutsk
- (GMT+09:30)Adelaide
- (GMT+09:30)Darwin
- (GMT+10:00)Brisbane
- (GMT+10:00)Canberra, Melbourne, Sydney
- (GMT+10:00)Guam, Port Moresby
- (GMT+10:00)Hobart
- (GMT+10:00)Vladivostok
- (GMT+11:00)Magadan, Solomon Is., New Caledonia
- (GMT+12:00)Auckland, Wellington
- (GMT+12:00)Fiji, Kamchatka, Marshall Is.
- (GMT+13:00)Nuku'alofa

Figure 7-3 Administration - Time Settings page

The default address is pool.ntp.org. It synchronizes every day.

7.3.2 Disable Time Server

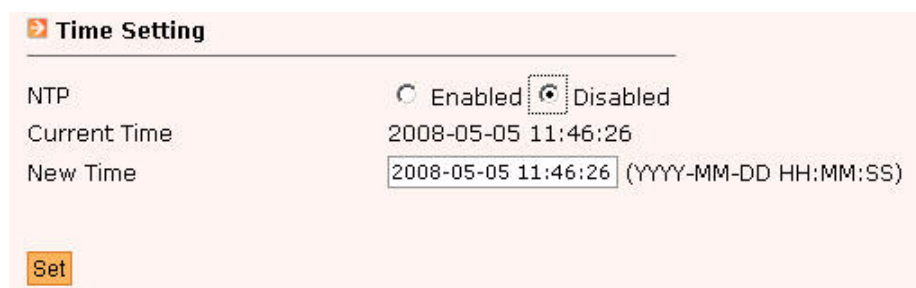
Select GS8 equipment's time zone in the drop-down list.

Note: Time zone is necessary if you use NTP service.

7.3.3 Change Time

Set time by yourself. The format is YYYY-MM-DD HH:MM:SS.

Note: Be carefule about the format.



Time Setting

NTP ☐ Enabled ☒ Disabled

Current Time 2008-05-05 11:46:26

New Time (YYYY-MM-DD HH:MM:SS)

Set

Figure 7-4 Administration - Time Settings - Time Setting page

Chapter 8

SMS

GS8 provides SMS route setting, client setting, receiving and sending management page at **SMS** menu.

Monitor	Line Settings	Call Settings	SMS	Administration	Maintenance	admin	Logout
2008-12-15 16:34							
Common Tasks Route GTXT Client Configuration Send Test Message Received Messages							
Description	Source	Destination	Caller Pattern	Callee Pattern			
	GSM/ALL	GTXT/3	ALL	ALL			
	IP/ALL	GTXT/3	ALL	ALL			
11	GSM/slot4,IP/1	IP/1	ALL	ALL			
Description Source Line GSM ☐ ALL ☐ slot4 IP ☐ ALL ☐ 1 Caller Pattern Callee Pattern Destination Line GSM ☒ slot4 IP ☒ 1 GTXT ☒ 2 ☐ 3 Alter Strategy Edit							
Add Modify Remove Move Down Move Up							

Figure 8-1 SMS settings page

8.1 Route

Click Route on the left task bar to set intellectual route for GS8 SMS sending.

Two parts in Route setting page:

- The above part: show existing SMS route list.
- The below part: edit area of SMS route

8.1.1 Route List

Description	Source	Destination	Caller Pattern	Callee Pattern
	GSM/ALL	GTXT/3	ALL	ALL
	IP/ALL	GTXT/3	ALL	ALL
11	GSM/slot4,IP/1	IP/1	ALL	ALL

Figure 8-2 SMS - Route List

- **Description:** the description of this route.
- **Source:** the type of source device and ports available.

Note: Source device matching is perfect matching, you may precall with the exactly matched route, refers to 6.3 Call Route

- **Destination:** the type of destination device and ports available
- **Caller Pattern:** caller number need to be matched for this rule, the default is 'ALL'
- **Callee Pattern:** callee number need to be matched for this rule, the default is 'ALL'

Choose one strategy and press **[Move Down]** or **[Move Up]** buttons to reorder the sequence. press **[Modify]** or **[Remove]** buttons to edit or delete this strategy.

8.1.2 Parameters Descriptions

Description		
Source Line	GSM ☐ ALL	☐ slot4
	IP ☐ ALL	☐ 1
Caller Pattern		
Callee Pattern		
	GSM ☐ slot4	
Destination Line	IP ☐ 1	
	GTXT ☐ 2	☐ 3
Alter Strategy	Edit	
Add Modify Remove Move Down Move Up		

Figure 8-3 SMS - Route setting page

- **Description:** the description of this route
- **Source Line:** the type of source device (includes FXO, GSM, CDMA, IP) and ports available (can be multi-chosen) , for example, 'Slot1-2' means the 2nd port of the 1st card. "G/C"means GSM or CDMA module: C-slot3 is the CDMA port of the third slot, "G-slot4" is the GSM port on the 4th slot.
- **Caller Pattern:** sender's number pattern, refers to 6.1 number matching rules, the default is all sender's number are valid.
- **Caller Pattern:** reveiver's number pattern, refers to 6.1 number matching rules, the default is all sender's number are valid.
- **Destination Line:** the type of destination device (includes FXO, CDMA , GSM, IP) and ports available(multi-chosen) , default 'ALL' means all ports of this card can be used.
- **Alter Strategy:** specific alter rules. For more details, see 6.3.3 number alter rules.

Note: In **Alter Strategy Settings**, it's composed of several sub-strategies (up to eight sub-strategies), and these sub-strategies are order-sensitive, please be careful about it.

	☐	Caller	Strip	Head	Parameter:
1	☐	Caller	Strip	Head	
2	☐	Caller	Strip	Head	
3	☐	Caller	Strip	Head	
4	☐	Caller	Strip	Head	
5	☐	Caller	Strip	Head	
6	☐	Caller	Strip	Head	
7	☐	Caller	Strip	Head	
8	☐	Caller	Strip	Head	

OK

Figure 8-4 Call Settings - Alter Strategy Settings page

- **Transform Objective:** caller or callee number.
- **Transform action:** includes Strip, Add, Keep, Replace, Calculate.
- **Transform location:** head or tail
- **Alter parameter:** digit number or specific number or string etc. press **[OK]** to save it and exit.

8.2 GTXT Client

GTXT is a Windows SMS receiver client especially developed for GS8. it interacts with GS8 via TCP connection. On the page of GTXT, you may check created GTXT account list , create and manage GTXT account information.

8.2.1 GTXT List

ID	Description	Username	Password
2	International User	USGTXT	USGTXT
3	Internal User	gtxt	gtxt

Figure 8-5 SMS - GTXT List

- **ID:** ID auto-assigned by system when create a GTXT Client account.

8.2.2 Parameters Descriptions

IP Settings

Description
Username
Password

Add
Modify
Remove

Figure 8-6 SMS - GTXT account setting

- **Description:** The description of GTXT Client account.
- **Username:** The user name of GTXT Client account.
- **Password:** The password of GTXT Client account.

Use **[Add]**, **[Modify]**, **[Remove]** buttons to manage GTXT Client account list in GS8 web management system.

8.3 Configuration

Set if receive, send and save SMS at **Configuration** page.

Setting

GTXT

GTXT Access ☒ Enabled ☐ Disabled

Listen Port

Update Request ☒ Accept ☐ Reject

Return Message

☒ If received within seconds, return to sender

Save Message

Which messages will be saved in GS8 when they can't be forwarded to destination

☐ None

☐ Messages From GSM

☐ Messages From SIP

☒ All Messages

Set

Figure 8-7 SMS setting page

- **GTXT**
 - **GTXT Accesss:** if use GTXT function.
 - **Listen Port:** listening port for GTXT user. The default is 8111, the value must be greater than 1024.
 - **Update Request:** if accept the request of updating received SMS from GTXT (if choose **Accept**, when GTXT Client requests update, GS8 should resend the SMSs saved on GS8 to GTXT)
- **Return Message:** GS8 provides SMS dynamic return function - GS8 return reply message to certain GTXT user within some valid time when it received a message from that GTXT user. At the same time, GS8 provides message saving function too - save the messages on GS8 when it got an un-sendable message for routing fail or unavailable destination. Then GS8 send certain GTXT user all his/her messages and deleted them locally after he/her login to GS8 and sending update request message. System administrator may set this return function at **Return Message** and set the valid time, count in second.
- **Save Message:** for failed message, GS8 provides saving locally function. you may set the message type which you want to save here:
 - **None:** Do not save failed message.
 - **Message From GSM:** save failed messages from GSM clients.
 - **Message From SIP:** save failed messages from SIP clients.
 - **All Messages:** save failed messages from all ports.

8.4 Send Test Message

On the page of **Send Test Message**, administrator may send test message here:

The screenshot shows a web form for sending SMS. It includes a 'To:' section with a dropdown menu for 'OutLine' (set to 'GSM/slot4') and a text field for 'Receiver Number' (filled with '13901210002'). An 'Add' button is next to the number field. Below this, the selected line and number are displayed as 'Line:GSM/slot4 To:13901210001' with a 'Remove' link. A large text area for 'Contents' is provided, with a character count 'Max 140 chars 0 chars' at the bottom. A 'Send Test Message' button is at the bottom of the form.

Figure 8-8 SMS - sending test page

Operate like below:

1. Choose a send port: set message sending line at **OutLine**. Available lines are preset at **Line Settings** menu.
2. Add destination phone number or IP phone number:
 - a. Input **Receiver Number**.
 - b. Press **[Add]** to confirm the number.

Repeat a, b steps to add up to 5 destination phone numbers. use [Remove] to delete created number.
3. Input test content at **Contents**, not more than 140 characters.
4. Ppress **[Send Test Message]** to send this message.

8.5 Received Messages

Check and do some simple operations on all saved messages at **Received Message**.

Figure 7-9 SMS saving setting page

The page of Received Message has two parts: list area and display area.

No.	Sender	In Line	Time
-----	--------	---------	------

Contents

Download Remove All

Figure 8-9 SMS Received Message page

8.5.1 View SMS

Click one message on the list of **Received Message** and read it at **Contents** field.

8.5.2 Download SMS

Use **[Download]** on the bottom of **Received Message** page to save all saved messages in GS8 locally as saved_sms.txt.

8.5.3 Remove SMS

Use **[Remove All]** on the bottom of the page of **Received Message** to delete all buffered messages on GS8.

Chapter 9

Maintenance

In **Maintenance** menu, administrators can maintain the system via backup, recovery, up-grade etc. operations.

9.1 System Reboot

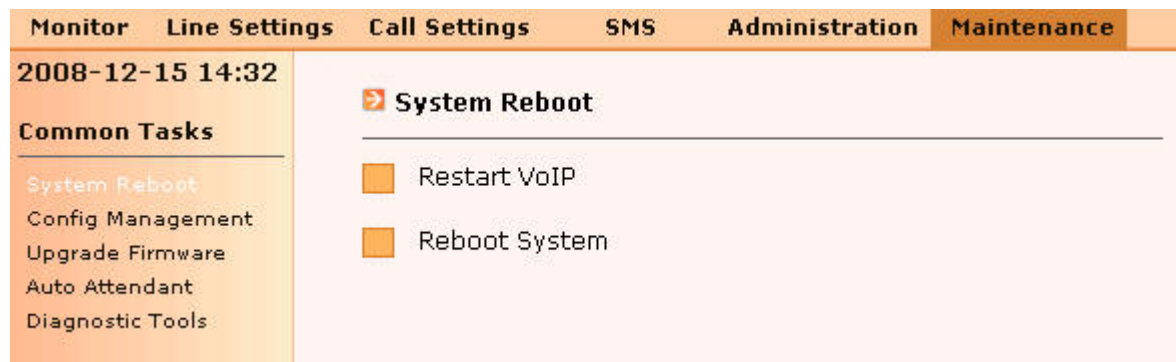


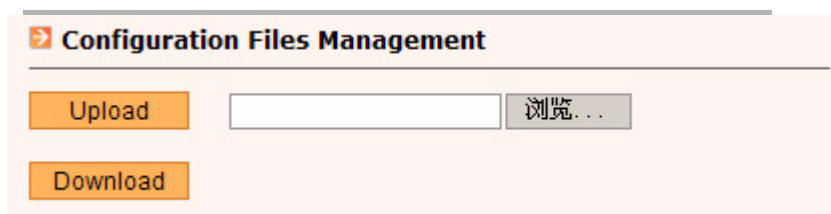
Figure 9-1 System Reboot page

- **Restart VoIP:** stop and restart the service.
- **Reboot System:** reboot the operating system of the equipment which will cut off all calls, then start the server and reload all datas again.

9.2 Config Management

9.2.1 Configuration File Mangement

Config management provides you the configuration's download and recovery.



Config Management page

- **Upload:** press **[Upload]** button to upload the backup configuration file to GS8 equipment.
- **Download:** press **[Download]** button to download system configuration as gs8_config.tgz file to local machine.

9.2.2 Reset To Default Factory Configurations

This menu will reset the equipment to the default factory configurations except network setting.

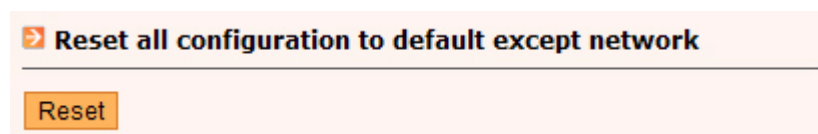


Figure 9-2 Reset to Default Factory Configurations page

9.3 Upgrade Firmware

Note: Keep the power on during upgrading.

Upgrade as these:

1. Keep the new file in local machine.
2. login to Web Management System, visit **Maintenance > Upgrade Firmware** setting page:

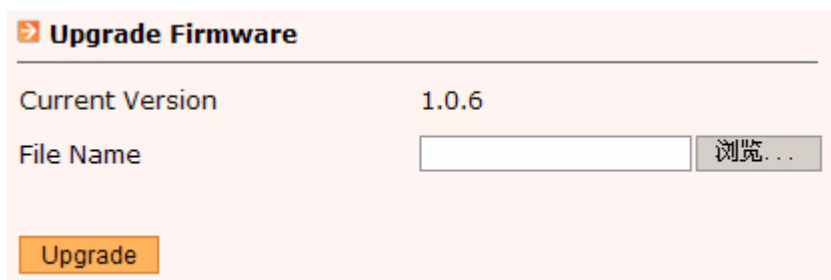


Figure 9-3 Upgrade Firmware page

3. Press **[View]** button to select the .img file.
4. Press **[Upgrade]** button to upgrade.

Note: If GS8 can not work because of the exception appeared during upgrade progress, please use 'GS8 Disaster Recovery System' to restart and upgrade GS8 again.

9.4 Auto Attendant

GS8 provides voice file uploading function. on the page of **Maintenance > Auto Attendants**, you may set language of prompts, and upload new voice file or recovery them to the defaults.

The screenshot shows the 'Maintenance - AA setting page' with three distinct sections, each with a title and a horizontal line separator:

- Voice Prompts Language:** Contains a label 'Select Voice Prompts Language', a dropdown menu currently set to 'English', and an orange 'Set' button below it.
- Upload Greeting Message:** Contains a label 'Voice Prompts File' next to a text input field and a '浏览...' (Browse...) button. Below this is a label 'Encode Type' next to a dropdown menu set to 'ulaw', and an orange 'Upload' button.
- Reset all voice prompts to default:** Contains an orange 'Reset' button.

Figure 9-4 Maintenance - AA setting page

9.4.1 Language Setting

You may set language for voice prompts at **Voice Prompts Language**. GS8 supports English and Chinese now.

9.4.2 Upload Prompts

Upload AA prompts (Greeting Message) files at **Upload Greeting Message** menu and define voice codec type for uploaded files.

1. Set **Voice Prompts File**: press **[View]** to choose a voice file.

2. Set **Encode Type**: define codec type for uploading file.
3. Press **[Upload]** to upload the file.

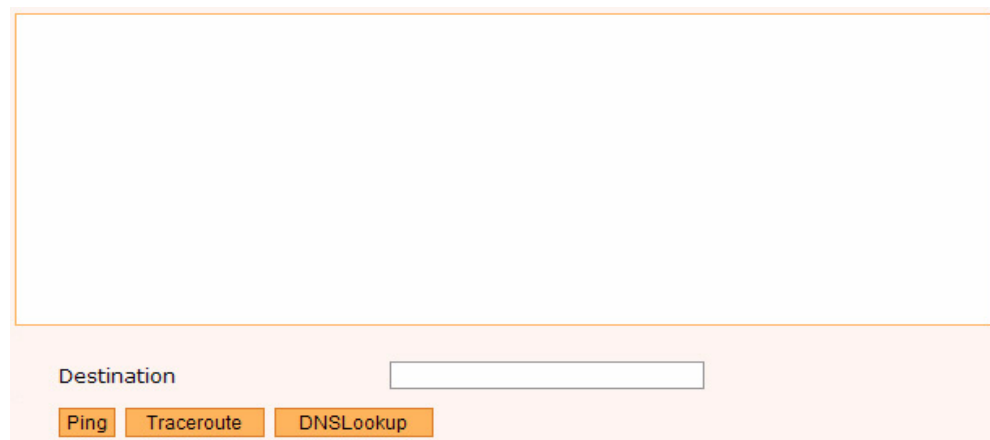
9.4.3 Recovery to Default Prompts

Press **[Reset]** on the page of **Reset all voice prompts to default** to recovery prompts to the defaults, which means clear all files uploaded by users and use the default prompts.

9.5 Diagnostic Tools

Visit **Maintenance > Diagnostic tools** menu and see this page (figure 8-5).

This page provides Ping, Traceroute and DNS Lookup diagnostic tools.



The screenshot shows a web interface for diagnostic tools. It features a large, empty rectangular box with an orange border, intended for displaying the results of the diagnostic tests. Below this box is a light pink footer area containing a 'Destination' label, a text input field, and three orange buttons labeled 'Ping', 'Traceroute', and 'DNSLookup'.

Figure 9-5 Maintenance - Diagnostic Tools page

- **Ping**: verify the connection with remote machine.
 - a. Input IP address and domain in address field.
 - b. Press **[Ping]** button and show this:
- **Traceroute**: Confirm the route to objective machine by tracking a message from source machine to objective machine.
 - a. Input domain name in the address field.
 - b. Press **[Traceoute]** button and get the result of tracking.
- **DNS Lookup**: Parsing domain name to IP address.
 - a. Input domain name in address field.
 - b. Press **[DNSLookup]** button and get the result of parsing.

Note: You need to set DNS server before you use DNSLookup tool.

Appendix A

GS8 Disaster Recovery System

If exception appears during normal upgrading progress and makes GS8 broken down, you can re-upgrade it via GS8 Disaster Recovery System.

The steps are:

1. Press Reset button for 3 seconds after power on.
2. Press Reset button for 2 seconds to enter GS8 Disaster Recovery System. The indicator light is red now.

Note: All datas in GS8 Disaster Recovery System are default configurations, you need to update configurations to use GS8. the default IP address is 192.168.0.100.

You can access GS8 Disaster Recovery System via login to Web Management System and re-upgrade GS8. (see 9.4 Upgrade Firmware) .

Appendix B

Glossary

10BaseT. A physical media specified by the IEEE 802.3 standard for supporting Ethernet with a maximum transmission rate of 10 Mb/s. 10BaseT consists of copper twisted-pair cable normally used for wiring ordinary telephones. Ethernet is a common technology used for connecting computers into a local area network (LAN).

100BaseT. A local area network transmission standard that supports a data rate of 100 Mb/s. Also known as *Fast Ethernet*, similar in function to 10BaseT.

Address Resolution Protocol (ARP). Defines the process of mapping an Internet Protocol address (IP address) to a physical machine address recognized in the local network. An *ARP table* maintains the correlation between each MAC address and its corresponding IP address within a network. ARP provides the protocol rules for defining this correlation and converting addresses in both directions. ARP is described by RFC 826.

Advanced Intelligent Network (AIN). A telephone network architecture that separates service logic from switching equipment. AIN encourages competition among service providers by allowing the addition of new services without requiring the re-design of existing switches.

Authentication. The process of ensuring that digital data transmissions are delivered to the intended receiver. Authentication also assures the receiver of the integrity of the message content and source. The simplest authentication method requires a user name and password to gain access to a specified account. Authentication protocols can be based on secret-key encryption or on public-key systems using digital signatures.

Authorization. The process of verifying the identity of a person or device. Authentication is commonly performed through logon passwords. Knowledge of the password is assumed to guarantee that the user authenticity. Internet business and many other transactions may require a more stringent authentication process, such as the use of digital certificates issued and verified by a Certificate Authority as part of a public key infrastructure. Logically, authentication precedes authorization, although they may often seem to be combined.

Bridge. A device that connects network segments that use the same protocol, such as Ethernet. A bridge forwards traffic between network segments on the basis of data link layer information. These segments would require a common network layer address.

Called Party. The person or device that receives a phone call or data transmission.

Calling Party. The person or device that initiates a phone call or data transmission.

Contact. A device where a user can be reached.

Decryption. Decryption is the process of converting encrypted data to its original form. See Encryption.

De-Militarized Zone (DMZ). A computer host or small network placed between a company's private network and the outside public network to prevent outside users from gaining direct access to a server that contains company data. The term is derived from the geographic area between two opponents where fighting is prohibited. A DMZ is an optional, more secure approach to a firewall and effectively acts as a proxy server as well.

Direct Inward Dialling (DID). DID is a service that allows users that are connected to a common server (such as a media exchange or a PBX) to receive calls from sources external to the server without the intervention of an auto attendant or operator. Under DID, each user is assigned a unique telephone number, as opposed to the typical PBX setup that assigns extensions that are based on a common telephone number.

Domain Name System (DNS). Defines the manner that the Internet translates names of network nodes into addresses. SIP uses DNS to resolve the host names of endpoints to IP addresses.

Dynamic Host Configuration Protocol (DHCP). A communication protocol that defines a method where network administrators manage and automate Internet Protocol (IP) address assignment within an enterprise network. DHCP allows you to move network devices from one subnet to another without administrative attention. If using DHCP, you can connect IP phones to the network and become operational without having to manually assign an IP address and additional network parameters. The ZIP 4x4 phone complies with the DHCP specifications documented in RFC 2131 and are DHCP-enabled by default.

Advanced Encryption Standard (AES). Also known as Rijndael, this is a block cipher adopted as an encryption standard by the U.S. government and developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen. It has been analyzed extensively and is now used widely worldwide as a replacement for its predecessors the Data Encryption Standard (DES) and the triple DES (3DES). AES was announced by the NIST on 26 November 2001 after a 5-year standardization process and became a standard on 26 May 2002. It is one of the most popular algorithms used in symmetric key cryptography and is acceptable by the US government for classified information up to Top Secret.

Encryption. The process of converting data into a form that can be read only by the intended receiver. Decryption is the process of converting encrypted data to its original form. Traditional encryption schemes utilize the same key to encrypt and decrypt data. Public-key encryption schemes require two keys: a public key, which anyone may use, and a corresponding private key, which is possessed only by the person who created it. With this method, anyone may send a message encrypted with the owner's public key, but only the owner has the private key necessary to decrypt it. PGP (Pretty Good Privacy) and DES (Data Encryption Standard) are two of the most popular public-key encryption schemes.

Ethernet. The most widely-installed local area network (LAN) technology. Originally developed at the Xerox Corporation Palo Alto Research Center, Ethernet is specified in the IEEE 802.3 standard. Ethernet is a best-effort delivery system that uses CSMA/CD technology. Ethernet can be run over a variety of physical media, including coaxial, twisted pair, and fiber optics.

Firewall. A device, located at a network gateway server, that protects the resources of a private network from external entities. Typically comprises a set of related programs or a dedicated computer equipped with such security features as logging, reporting, alarms, and a control mechanism.

File Transfer Protocol (FTP). An application layer standard Internet protocol that uses the TCP/IP protocols to exchange files between computers on the internet. Commonly used to transfer web page files from the creator to a server or to download programs and other files from a computer to other servers. Described by RFC 959.

Foreign Exchange Office (FXO). An analog interface that connects to the Public Switched Telephone Network (PSTN) central office and is the interface offered on a standard telephone.

Foreign Exchange Station (FXS). An analog interface that connects directly to a standard telephone and supplies ring, voltage, and dial tone.

FTP Account. An SE system identifier that points to an FTP address.

Fully Qualified Domain Name (FQDN). The portion of an Internet URL that identifies the server program that an Internet request addresses. The FQDN includes the second-level domain name (such as Zed-3.com) and any other levels (such as www.Zed-3.com).

Gateway. A network point that serves as an entrance to another network. Computers that control traffic within an enterprise's network or at the local Internet Service Provider (ISP) are gateways. IP datagrams are transferred from network to network through gateways until it reaches its final destination. See Router.

Hub. A hub network topology consists of a backbone (main circuit) to which a number of outgoing lines can be attached, each providing at least one connection port for attaching devices. As a network product, a hub may include a group of modem cards for dial-in users, a gateway card for connections to a local area network, and a line connection.

Hypertext Transfer Protocol (HTTP). An application layer protocol that defines a set of rules for exchanging files (text, images, sound, video, and other multimedia files) on the Internet. Described by RFC 2068.

Incoming call. A call originated by a source that is external to the enterprise.

Internet. A worldwide computer network system in which users at any one computer can, with permission, exchange information from any other computer and sometimes talk directly to users at other computers. also known as the "Net." Originally designed by the Advanced Research Projects Agency (ARPA) of the U.S. Defense Department in 1969 so that a communication signal could withstand a nuclear war and serve military institutions worldwide. First known as the ARPAnet, the internet has evolved into public, cooperative, and self-sustaining facility accessible to billions of people worldwide.

Internet Control Message Protocol (ICMP). A message control and error-reporting protocol between a host server and an Internet gateway that enables hosts to send error or control messages to other hosts. ICMP is an integral part of IP and must be implemented by every IP module. Instances for sending an ICMP message include datagram processing errors, the datagram cannot reach its destination, or when the gateway has insufficient buffering capacity to forward a datagram. The ZIP 4x4 phone supports ICMP as documented in RFC 792.

Internet Engineering Task Force (IETF). The organization that defines standard Internet operating protocols such as TCP/IP. The IETF is supervised by the Internet Society Internet Architecture Board (IAB). IETF members are drawn from the Internet Society's individual and organization membership. Standards are expressed in the form of Requests for Comments (RFCs).

Internet Key Exchange (IKE). The method for exchanging encryption and authentication keys over an unsecured medium, such as the Internet.

Internet Protocol (IP). A network layer protocol that sends datagram packets between Internet nodes. IP is a connection-less protocol, implying that there is no continuing connection between communicating endpoints. IP provides addressing, type-of-service (ToS) specification, security, fragmentation and reassembly features. The most widely used IP version is Internet Protocol Version 4 (IPv4). The ZIP 4x4 phone supports IP as defined in RFC 791.

Internet Protocol Version 6 (IPv6). The latest level of the IP that is included in many projects, including the major computer operating systems. The most obvious improvement in IPv6 over IPv4 is the lengthening of IP addresses from 32 bits to 128 bits. All servers that support IPv6 will also support Internet Protocol Version 4.

Intranet. A restricted-access network that works like the Web, but isn't on it. Usually owned and managed by a corporation, an intranet enables a company to share its resources with its employees without making available confidential information to everyone with Internet access.

IP Address (version 4). A 32-bit number that identifies each sender or receiver of information sent across the internet. An IP address has two parts: the network identifier and the identifier of a specific device on the network. On the Internet itself – between the router that moves packets between points along the route – only the network part of the address is examined.

IP Security (IPSec). Security standard produced by the Internet Engineering Task Force (IETF). a protocol suite that provides all necessary elements for secure communications-authentication, integrity, and confidentiality-and makes key exchange practical even in larger networks.

Jitter. Jitter is the deviation in some aspect of the pulses in a high-frequency digital signal or the period frequency displacement of the signal from its ideal location. The SE system utilizes Jitter Buffers to compensate for jitter.

Key Management. The management and handling private keys used for signing or encryption. The only reasonable way to protect the integrity and privacy of information is to rely upon the secure use of these keys, including the activities of selection, exchange, storage, certification, expiration, revocation, changing, and transmission. Most of the work in managing information security systems lies in the key management.

Lightweight Directory Access Protocol (LDAP). A software protocol that enables anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet. LDAP is a "lightweight" (smaller amount of code) version of Directory Access Protocol (DAP), which is part of X.500, a standard for directory services in a network. LDAP is lighter because, in its initial version, it did not include security features. Described by RFC 2251.

Load balancing. The mapping (or re-mapping) of work to processors, with the intent of improving the efficiency of a concurrent computation.

Local Area Network (LAN). A group of computers and associated devices that share a common communications line and the resources of a single processor or server within a limited geographic area, such as an office building. 10BaseT Ethernet is the most commonly used form of LAN. A hardware device called a hub serves as the common wiring point, enabling data to be sent from one machine to another over the network. LANs are typically limited to distances of less than 500 meters and provide low-cost, high-bandwidth networking capabilities within a small geographical area.

Media Access Control (MAC) Address. A hardware number that uniquely identifies a computer or other device. Within an Ethernet configuration, the MAC address is a 6-octet address assigned to the network interface card. When your computer is connected to the Internet, a correspondence

table relates your IP address to your computer's physical (MAC) address on the LAN. The MAC address is used by the Media Access Control sublayer of the Datalink Control (DLC) protocol layer. Each physical device type has a different MAC sublayer.

Network Address Translation (NAT). A standard for translating a secure IP address used within one network to a different IP address known from another network. In addition to providing Internet access for trusted networks with privately assigned IP addresses, NAT conserves on the number of global IP addresses required by a network because each machine in a network does not require a registered IP address.

Network Interface Card (NIC). A circuit board or card that is installed in a computer for the purpose of connecting the computer to a network. Personal computers on a LAN usually contain a NIC designed for a specific LAN transmission technology, such as Ethernet.

Network Time Protocol (NTP). A protocol that synchronizes computer clocks on an IP network. Described by RFC 1305.

Per-Hop Behavior. The differential treatment an individual packet receives while being routed through a network, as implemented by queue service or queue management disciplines. These per-hop behaviors are useful and required in network nodes to deliver differentiated treatment of packets regardless of end-to-end construction or intra-domain services. Per-Hop behavior is discussed in RFC 2474 and Per-Hop Identification codes are defined in RFC 3140.

Point-to-Point Protocol (PPP). A protocol that defines a communication method between two computers using a serial interface. Typically used to connect a personal computer to a server through a phone line.

Proxy Server. A server that acts as an intermediary between a workstation and the Internet to provide a caching service and ensure security and administrative control for the enterprise. The proxy server is invisible to the workstation. All Internet requests and returned responses involving the workstation appear to be directly with the addressed Internet server.

Public Switched Telephone Network (PSTN). The world-wide collection of voice-oriented public telephone networks. Also referred to as plain old telephone service (POTS).

Quality of Service (QoS). The concept that transmission rates, error rate, and other characteristics over a network or the Internet can be quantified, improved, and guaranteed (to a certain extent) in advance. QoS is particularly concerned with the continuous transmission of high-bandwidth video and multimedia data.

Real-Time Transport Control Protocol (RTCP). The protocol companion to RTP that provides error, session control, and identification data about a transport session. Described by RFC 1889.

Real-Time Transport Protocol (RTP). An Internet protocol standard that specifies a method for programs to manage the real-time transmission of multimedia data over unicast or multicast network services. RTP combines its data transport with a control protocol (RTCP), which makes it possible to monitor data delivery for large multicast networks. The ZIP 4x4 phone supports RTP as a media channel for voice and video applications as described in RFC 1889.

Repeater. A device that receives a digital signal on a transmission medium and regenerates the signal for the next leg of the medium. Repeaters overcome attenuation losses caused by free-space electromagnetic-field divergence or cable loss over electromagnetic media. A series of repeaters facilitates the extension of a signal over long distances.

Request for Comments (RFC). A formal document issued by the Internet Engineering Task Force. Some RFCs are informational in nature while others become Internet standards. RFCs are the result of committee drafting and subsequent review by interested parties. No further comments

or changes to an RFC are permitted once it becomes an Internet standard. changes to internet standards are enacted through subsequent RFCs that supersede or elaborate on all or parts of existing RFCs.

Reverse Address Resolution Protocol (RARP). A protocol by which a physical machine in a local area network can request its IP address from a gateway server's Address Resolution Protocol table or cache. RARP is described in RFC 903.

RJ-45. A single-line digital transmission interface. Resembling a standard phone connector, an RJ-45 connector is twice as wide (with eight wires) and is used for connecting computers to local area networks (LANs) or phones with multiple lines.

Router. A device that determines the next network point to which a data packet should be sent on the to its final destination. Routers also act as traffic cops, allowing only authorized machines to transmit data into the local network so that private information can remain secure. In addition to supporting these dial-in and leased connections, routers also handle errors, maintain network usage statistics, and handle security issues.

Routing Information Protocol (RIP). A widely used protocol for managing router information within a self-contained network, such as a corporate LAN. A gateway host sends its entire routing table to its closest neighbor every 30 seconds, which in turn passes the table to its neighbor. this process is repeated until all hosts in the network have the same information. RIP is described by RFC 1058.

Server. A computer program or device that provides services to other computers.

Session Description Protocol (SDP). An ASCII-based protocol that describes multimedia sessions and their related scheduling information, including information transport session participant port numbers and contact addresses. The ZIP 4x4 phone uses SDP for session descriptions as documented in RFC 2327.

Session Initiated Protocol (SIP). An Internet standard protocol that defines a method of initiating an interactive user session involving multimedia elements, such as voice, chat, gaming, video, and virtual reality. SIP is a request-response protocol that deals with requests from clients and responses from servers through any transport protocol, such as UDP or TCP. Described by RFC 3261, SIP can establish, modify, or terminate multimedia sessions or Internet telephony calls.

Simple Network Management Protocol (SNMP). The protocol that governs network management and the monitoring of network devices and their functions. SNMP is described formally in RFC 1157 and in a number of related RFCs.

Simple Network Time Protocol (SNTP). A protocol that synchronizes computer clocks on an IP network. Similar to NTP with fewer features. Some IP phones use SNTP for their date and time synchronization functions. Described by RFC 2030.

SIP Endpoint. An internet host that understands the SIP protocol.

SIP Registrar. A SIP Registrar is a UAS that responds to REGISTER requests and maintains a list of bindings that are accessible to proxy servers and redirect servers within its administrative domain.

SIP Server. A network device that performs special functions at the request of SIP endpoints. Servers typically act in response to SIP endpoint requests, but can also initiate functions on their own. RFC 3261 defines three types of SIP servers: SIP Proxy servers, Redirect servers, and Registrar servers.

Subnet Mask. A number that, when applied to an IP address, can identify the subnetwork where the address resides. For example, within a class B network, a subnet mask of 255.255.255.0 specifies that the first two portions of the decimal dot format are the network number, while the third portion is a subnet number. The fourth portion is the host number. A subnet mask of 255.255.0.0 specifies a class B network that does not have a subnet.

Switch. A network device that selects a path or circuit for sending a unit of data to its next destination. A switch may also include the function of the router. A switch is generally a simpler and faster mechanism than a router, which requires knowledge about the network and how to determine the route. A switch is usually associated with layer 2 of the OSI communications model.

Transmission Control Protocol (TCP). A set of communications protocols that, when used with Internet Protocol (IP), support peer-to-peer connectivity functions for both local and wide area networks. TCP/IP is a communications protocol which allows computers with different operating systems to communicate with each other and controls how data is transferred between computers on the Internet. While IP handles the actual delivery of data, TCP tracks the data packets into which a message is divided for efficient routing through the internet. The ZIP 4x4 phone supports TCP as described by RFC 793.

Trivial File Transfer Protocol (TFTP). An Internet software utility for transferring files that, while simpler to use than FTP, provides fewer features. TFTP is used where user authentication and directory visibility are not required. The ZIP 4x4 phone uses TFTP to download configuration files and software updates from the TFTP Server, as described in RFC 1350.

Trunk Port. A device that allows a switch to bundle traffic from several VLANs through a single physical port, sorting the various packets by the VLAN identifier (VID) in their frame headers.

Trusted Network. Networks inside your network security perimeter. Only known and approved sources are allowed access to a trusted network.

Tunnelling. The transmission of data intended for use only within a private network through a public network in such a way that the routing nodes in the public network are unaware that the transmission is part of a private network. Tunneling is generally done by encapsulating the private network data and protocol information within the public network transmission units so that the private network protocol information appears to the public network as data. Tunneling allows the use of the Internet, which is a public network, to convey data on behalf of a private network.

Universal Resource Locator (URL). A standard method of specifying the location of an internet resource. Also referred to as a location or address, URLs specify the location of files on servers. A general URL has the syntax protocol://address. For example, <http://www.Zed-3.com/index.htm> specifies that the protocol is http and the address is www.Zed-3.com/index.htm.

Unshielded Twisted Pair (UTP). Also known as 10BaseT. This is the standard cabling used for telephone lines. It is also used for Ethernet connections.

Untrusted Network. Networks that are outside of your security perimeter. Private and shared networks over which you have no control over the administration or security policies. Firewalls deal with the problem of communicating with these networks while protecting your trusted network.

User Agent. A SIP logical entity that can act as both a user agent client (UAC) and user agent server (UAS). The role of UAC and UAS, as well as proxy and redirect servers, are defined on a transaction-by-transaction basis. For example, the user agent initiating a call acts as a UAC when

sending the initial INVITE request and as a UAS when receiving a BYE request from the calling station. Similarly, the same software can act as a proxy server for one request and as a redirect server for the next request.

User Agent Client. A SIP logical entity that creates a new request, and then uses the client transaction state machinery to send it. The role of UAC lasts only for the duration of that transaction. If a piece of software initiates a request, it acts as a UAC for the duration of that transaction. If it receives a request at a later time, it assumes the role of a user agent server to process that transaction.

User Agent Server. A SIP logical entity that generates a response to a SIP request. The response accepts, rejects, or redirects the request. This role lasts only for the duration of that transaction. If a piece of software responds to a request, it acts as a UAS for the duration of that transaction. If it generates a request later, it assumes the role of a user agent client to process that transaction.

User Datagram Protocol (UDP). A communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses IP. An alternative to TCP, UDP uses the IP to transfer a data unit between computers without dividing it into packets and reassembling it at the other end. Because UDP does not provide the sequencing of packets, the application program that uses UDP must be able to verify that the entire message has arrived in the proper order. UDP is in the Transport Layer (or Layer 4) of the OSI communication model. The ZIP 4x4 phone supports UDP as defined in RFC 768 for SIP signalling.

Virtual Local Area Network (VLAN). A Local Area Network that maps workstations on a logical basis (such as department or primary application) rather than by physical location. VLAN members are not identified by their location on a physical subnetwork but through the use of tags in the frame headers of their transmitted data. VLANs are described in the IEEE 802.1Q standard.

Virtual Private Network (VPN). A method of using the Internet to provide remote offices or individual users with secure access to their organization's network. A virtual private network can be contrasted with an expensive system of owned or leased lines that can only be used by one organization. The goal of a VPN is to provide an organization with the same capabilities, but at a much lower cost. VPNs are possible because of technologies and standards such as tunneling, screening, encryption, and IPSec.

Wide Area Network (WAN). A geographically dispersed telecom network. Although a WAN may be privately owned, the term usually implies the inclusion of public networks.